	Georgia Technology Authority	
Title:	**Media Sanitization - Vendor Return**	
PSG Number:	SS-08-035.01	**Topical Area:** Security
Document Type:	Standard	**Pages:** 3
Issue Date:	3/31/08	**Effective Date:** 3/31/08
POC for Changes:	GTA Office of Information Security	
Synopsis:	Establishes standards for sanitization and disposal of all electronic media subject to vendor return.	

PURPOSE

With the advanced features of today's operating systems, electronic media used on a system should be assumed to contain information commensurate with the security categorization of the system's confidentiality. If not handled properly, release of these media outside state control could lead to an occurrence of unauthorized disclosure of information.

Sanitization mitigates the risks of unauthorized disclosure of sensitive information by ensuring that data deleted from systems being returned to vendors or manufacturers cannot be easily recovered or reconstructed.

SCOPE, AUTHORITY, ENFORCEMENT, EXCEPTIONS

See Enterprise Information Security Charter (Policy)

STANDARD:

All storage media (magnetic, optical, electrical, or other) subject to vendor return agreements (such as but not limited to lease, warranty, rebate/refund etc.) shall have an acceptable means to appropriately sanitize (clear, purge) the media of all residual data in accordance with state and agency requirements prior to return to vendor.

Electronic media shall be classified commensurate with the highest level of information processed on the system for which it was used in accordance with the Data Categorization standard.

Acquisitions that include vendor return provisions shall make allowances for the agency to retain media used to process data categorized as HIGH. Media categorized as HIGH shall be destroyed in accordance with DOAS Equipment Disposal Policy when no longer needed.

Non-disclosure statements shall be required of vendors providing off-site hardware maintenance and agencies shall establish appropriate media handling and protection procedures in accordance with the Media Handling and Protection standard.

Only digital media used for processing data categorized as Low or Moderate shall be eligible for sanitization and reuse outside agency control Standard.

Sanitization or destruction of all electronic media shall be documented and certified, in writing, by the Agency head or designee before return to the vendor in accordance with the Disposal of E-Surplus Media standard.

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

- Media Controls (Policy)
- Surplus Electronic Media (Standard)
- Media Protection and Handling (Standard)
- Data Categorization – Impact Level (Standard)

REFERENCES

- DOAS Electronic Equipment Disposal (Policy)
- NIST 800-88 Guidelines Media Sanitization
- NIST 800-36 Guide to Selecting Information Technology Security Products

TERMS and DEFINITIONS

Electronic Media – Any electronic equipment that uses non-volatile memory to store data. Examples includes but is not limited to: Desktop computers, laptop/notebook computers, network servers, network storage devices, PDAs, network routers and switches, digital copiers, scanners, printers, faxes, and all forms of optical and magnetic storage media.

Non-volatile memory - Computer memory that can retain the stored information even when not powered. Examples of non-volatile memory include read-only memory, flash memory, most types of magnetic computer storage devices (e.g. hard disks, floppy disk drives, and magnetic tape), optical disc drives, and early computer storage methods such as paper tape and punch cards.

Sanitization - Refers to the general process of removing data from storage media, such that there is reasonable assurance that the data may not be easily retrieved and reconstructed.

Clear – A level of media sanitization that would protect the information against a robust keyboard attack. Clearing must render the information irretrievable by data, disk or file recovery utilities. It must be resistant to keystroke recovery attempts and data scavenging tools. (example: overwriting)

Purge – Media sanitization process that protects information against a laboratory attack using non-standard systems to conduct data recovery attempts on media outside their normal operating environment. (example: degaussing)

Destruction – Ultimate form of sanitization. Media cannot be reused as originally intended and any residual medium should withstand a laboratory attack. (examples: incineration, melting, shredding)

Certification – Refers to the process of verifying that media has been sufficiently sanitized and/or destroyed and methods used satisfactorily meet requirements.

Reuse – To use again for the same or different purposes such as resale, donate, vendor return, refurbish, etc.

Note: The PSG number was changed from S-08-035.01 on September 1, 2008